Signatures of non-classicality in mixed-state quantum computation

Animesh Datta[1,2] and Sevag Gharibian[3]

[1]*Institute for Mathematical Sciences, 53 Prince's Gate, Imperial College, London, SW7 2PG, UK*
[2]*QOLS, The Blackett Laboratory, Imperial College London, Prince Consort Road, SW7 2BW, UK*
[3]*Institute for Quantum Computing, University of Waterloo, Waterloo, Canada*

(Dated: April 18, 2009)

We investigate signatures of non-classicality in quantum states, in particular, those involved in the DQC1 model of mixed-state quantum computation [Phys. Rev. Lett. **81**, 5672 (1998)]. To do so, we consider two known non-classicality criteria. The first quantifies disturbance of a quantum state under locally noneffective unitary operations (LNU), which are local unitaries acting invariantly on a subsystem. The second quantifies measurement induced disturbance (MID) in the eigenbasis of the reduced density matrices. We study the role of both figures of non-classicality in the exponential speedup of the DQC1 model and compare them *vis-a-vis* the interpretation provided in terms of quantum discord. In particular, we prove that a non-zero quantum discord implies a non-zero shift under LNUs. We also use the MID measure to study the locking of classical correlations [Phys. Rev. Lett. **92**, 067902 (2004)] using two mutually unbiased bases (MUB). We find the MID measure to exactly correspond to the number of locked bits of correlation. For three or more MUBs, it predicts the possibility of superior locking effects.

PACS numbers: 03.65.Ud,03.67.Mn,03.67.Lx
Keywords: Quantum discord, DQC1, Locking

I. INTRODUCTION

A thorough understanding of classical and quantum correlations underlies their successful exploitation in quantum information science. The relative roles and abilities of these two forms of correlations in performing specific computational and information processing tasks would be a valuable advance in the field. Substantial progress in this direction have already been achieved. The role of entangled states in quantum information processing and computing is quite well studied. Jozsa and Linden [1] showed that multipartite entanglement must grow unboundedly with the problem size if a pure-state quantum computation is to attain an exponential speedup over its classical counterpart. In the context of information processing, Masanes has shown [2] that all bipartite entangled states can enhance the teleporting power of some other state. In spite of these successes, there are instances of quantum computations where the quantum advantage cannot be attributed to entanglement. Meyer has presented a quantum search algorithm that uses no entanglement [3]. Instances are also known of oracle based problems that can be solved without entanglement, yet with certain advantages over the best known classical algorithms [4],[5].

Given this scenario, it becomes a logical necessity to study the essentialness of entanglement in quantum information science. The oldest signature of quantum behavior has been nonlocality. Interestingly, it is well known that quantum nonlocality and entanglement are not equivalent notions [6],[7]. Entanglement stems from the superposition principle, or the amplitude description of quantum mechanics. This description is, however, not one that uniquely defines quantum mechanics. Consequently, it should not be a surprise that entanglement cannot capture the whole power of quantum mechanics. This provides a significant motivation for studying alternative certificates of quantum behavior.

A much more realistic motivation is that provided by mixed-state quantum computation. Pure states in a quantum computation inevitably get mixed due to decoherence. Countering this requires the techniques of quantum error-correction. A different way to address this issue would be to study the prospects of quantum computational speedup with mixed states themselves [8]. NMR quantum computation provides a perfect scenario for this. As a simplified model for this, Knill and Laflamme proposed the DQC1 or the 'power of one qubit' model [9]. Though not believed to be as powerful as a pure-state quantum computer, it is known to provide an exponential speedup over the best known classical algorithm for estimating the normalized trace of a unitary matrix. The DQC1 model was found to have a limited amount of (bipartite) entanglement that does not increase with the system size. Additionally, for certain parameter settings, there is no distillable entanglement present whatsoever, and yet the model retains its exponential advantage. In this latter case the state has a positive partial transpose, and thus possesses, at most, just bound entanglement [10]. Looking for a more satisfactory explanation for the exponential speedup, the quantum discord [11],[12] was calculated, of which the amount found was a constant fraction of the maximum possible [13], regardless of the parameter settings for the model. In this paper, we study two alternative methods of studying the quantum behavior of the DQC1 model.

Locally noneffective unitary operations (LNU) have previ-

ously been studied with the aim of developing an entanglement detection criterion [14],[15]. Here, we study the LNU as a possible notion of non-classicality, motivated by the disturbance of a quantum state under unitary operations. We provide a brief introduction to the LNU in Sec II. In Sec III, we employ LNU in analyzing the DQC1 model. The DQC1 model has previously been studied using the quantum discord. Thus, in Sec IV, we compare these two certificates of non-classicality, with the aim of contrasting *disturbance under measurement* with *disturbance under unitary operations*. We then move on to study the DQC1 model using the measurement-induced disturbance (MID) measure [16] in Sec V. In Ref. [16], a preliminary analysis of the DQC1 model was begun. Here, we extend this analysis to the entire parameter range for the DQC1 model, including those which limit the DQC1 state to being at most bound entangled. This latter case is of particular interest due to the lack of distillable entanglement. Later, in Sec V B, we present an example in the realm of quantum communication where the MID measure is a good certificate of non-classicality. Specifically, we study the construction of Ref. [17] which uses two mutually unbiased bases (MUB) to lock classical correlations in a quantum state. The value of the MID measure in this case is exactly the number of locked bits of correlation in the state. Considering the same construction with more than two MUBs, the MID measure portends superior locking abilities, though they must involve MUBs more general than those based on Latin squares and generalized Pauli matrices [18]. We conclude with a brief discussion in Sec VI.

Throughout, we denote a vector by $\boldsymbol{v}$, and take all logarithms to base 2. We define $D(\mathcal{H}^M \otimes \mathcal{H}^N)$ as the set of density operators acting on the MN-dimensional Hilbert space $\mathcal{H}^M \otimes \mathcal{H}^N$. All designations of a density matrix without any subscripts will be implied to mean a bipartite state. For example, τ shall stand for τ_{AB}.

II. LOCALLY NONEFFECTIVE UNITARY OPERATIONS (LNU)

We begin by introducing locally noneffective unitary operations (LNU), first proposed under the name local *cyclic* operations [14]. For this, consider a bipartite quantum state $\rho \in D(\mathcal{H}^M \otimes \mathcal{H}^N)$, shared between A and B such that $\rho_A = \mathrm{Tr}_B(\rho)$ and $\rho_B = \mathrm{Tr}_A(\rho)$. Suppose now that Alice performs a local unitary U_A that does not change her subsystem, that is, $\rho_A = U_A \rho_A U_A^\dagger$, or equivalently

$$[\rho_A, U_A] = 0. \tag{1}$$

This action can, however, affect the state of the total system, such that if we define $\rho_f := (U_A \otimes \mathbb{I}_B)\rho(U_A \otimes \mathbb{I}_B)^\dagger$, it is possible that $\rho \neq \rho_f$. Unitaries satisfying Eqn. (1) are called LNU [14]. To quantify the difference between ρ and ρ_f, we use

$$\begin{aligned} \mathrm{d}_{\max}(\rho) &:= \max_{\substack{U_A : \\ [\rho_A, U_A]=0}} \frac{1}{\sqrt{2}} \| \rho - \rho_f \|_{\mathrm{F}} \\ &= \max_{\substack{U_A : \\ [\rho_A, U_A]=0}} \sqrt{\mathrm{Tr}(\rho^2) - \mathrm{Tr}(\rho\rho_f)}. \end{aligned} \tag{2}$$

where $\| A \|_{\mathrm{F}} = \sqrt{\mathrm{Tr}(A^\dagger A)}$ denotes the Frobenius norm. From the latter expression, it is clear that $0 \leq \mathrm{d}_{\max}(\rho) \leq 1$. For any product state $\rho_{prod} := \rho_A \otimes \rho_B$, $\mathrm{d}_{\max}(\rho_{prod}) = 0$. Closed form expressions for $\mathrm{d}_{\max}(\rho)$ are known for (pseudo)pure states and Werner states [15]. As with the quantum discord, it is possible to have $\mathrm{d}_{\max}(\rho_{sep}) > 0$ for certain separable states, implying $\mathrm{d}_{\max}(\rho)$ is not a non-locality measure. A separable state $\rho_{sep} \in D(\mathcal{H}^M \otimes \mathcal{H}^N)$ is defined as one of the form

$$\rho_{sep} := \sum_k p_k |a^k\rangle\langle a^k| \otimes |b^k\rangle\langle b^k|, \tag{3}$$

where $\sum_k p_k = 1$, and the $|a^k\rangle \in \mathcal{H}^M$ and $|b^k\rangle \in \mathcal{H}^N$ are vectors of Euclidean norm 1. For two-qubit separable states, the maximum LNU distance attainable is [14]

$$\mathrm{d}_{\max}(\rho_{sep}) \leq \frac{1}{\sqrt{2}}. \tag{4}$$

As an illustration, the maximum LNU distance for the two-qubit isotropic state,

$$\rho_{iso} = \frac{1-z}{4} I_4 + z|\Psi\rangle\langle\Psi|, \qquad z \in [0,1] \tag{5}$$

where $|\Psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, is given by [15]

$$\mathrm{d}_{\max}(\rho_{iso}) = z. \tag{6}$$

By Eqn. (4), we can conclude that the two-qubit isotropic state is entangled for $z > 1/\sqrt{2}$. The partial transpose test, which in this case is necessary and sufficient, shows that this state is actually entangled for all $z > 1/3$, showing that the LNU distance is weaker at detecting entangled states than the former.

We remark that we have restricted our attention here to the case where the LNU is applied to subsystem A of ρ. Let us derive a simple upper bound on $\mathrm{d}_{\max}(\rho)$ which holds regardless of which target subsystem we choose, and which proves useful throughout this paper.

Theorem 1. *For any* $\rho \in D(\mathcal{H}^M \otimes \mathcal{H}^N)$,

$$\mathrm{d}_{\max}(\rho) \leq \sqrt{2\left(\mathrm{Tr}(\rho^2) - \frac{1}{MN}\right)}. \tag{7}$$

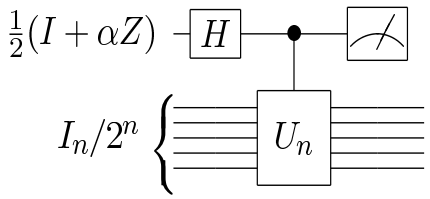

FIG. 1: The DQC1 circuit

Proof. Since $\| \rho - \frac{I}{MN} \|_{\rm F}$ is invariant under unitary operations, we have via the triangle inequality that:

$$\begin{aligned} \| \rho - \rho_f \|_{\rm F} &\leq \left\| \rho - \frac{I}{MN} \right\|_{\rm F} + \left\| \frac{I}{MN} - \rho_f \right\|_{\rm F} \\ &= 2 \left\| \rho - \frac{I}{MN} \right\|_{\rm F} \\ &= 2\sqrt{{\rm Tr}(\rho^2) - \frac{1}{MN}} \end{aligned} \tag{8}$$

Substituting this expression in Eqn. (2) gives the desired result. □

Thus, if the purity of a state ρ strictly decreases as a function of the dimension, then ${\rm d}_{\max}(\rho) \to 0$ as $MN \to \infty$.

III. LNU IN THE DQC1 MODEL

We now study the non-classical features of the DQC1 model of quantum computation, as quantified by ${\rm d}_{\max}(\rho)$. The $n+1$ qubit DQC1 state, as demonstrated in Fig (1), is given by [10]

$$\rho_{DQC1} = \frac{1}{2^{n+1}} \begin{pmatrix} I_n & \alpha U_n^\dagger \\ \alpha U_n & I_n \end{pmatrix}. \tag{9}$$

We will consider the top qubit to be system A on which our local unitary acts and the remaining n qubits as system B. The reduced state is then

$$\rho_A = {\rm Tr}_B(\rho_{DQC1}) = \frac{1}{2} \begin{pmatrix} 1 & \alpha\tau^* \\ \alpha\tau & 1 \end{pmatrix} \tag{10}$$

with $\tau = {\rm Tr}(U_n)/2^n$. For an arbitrary ${\rm SU}(2)$ unitary U_A acting on A, which we characterize as

$$U_A = \begin{pmatrix} e^{i\phi}\cos\theta & e^{i\chi}\sin\theta \\ -e^{-i\chi}\sin\theta & e^{-i\phi}\cos\theta \end{pmatrix}, \tag{11}$$

the LNU condition of Eqn. (1) requires that $\chi = \frac{\pi}{2} - \arg(\tau)$ and either $\phi = 0$ or $\theta = \pi/2$. Both cases lead to the same final expression, so set $\phi = 0$. Via Eqn. (2) and simple algebra, we hence have

$${\rm d}(\rho_{DQC1}, \theta) = \frac{\alpha \sin\theta}{2^{(n+1)/2}} \sqrt{1 - \frac{{\rm ReTr}(e^{-2i\arg\tau} U_n^2)}{2^n}}.$$

The now trivial maximization over all θ gives

$${\rm d}_{\max}(\rho_{DQC1}) = \frac{\alpha}{2^{(n+1)/2}} \sqrt{1 - \frac{{\rm ReTr}(e^{-2i\arg\tau} U_n^2)}{2^n}} \tag{12}$$

$$\leq \frac{\alpha}{2^{n/2}}. \tag{13}$$

Here, we have used the rough estimate ${\rm ReTr}(e^{2i\arg\tau} U_n^2) \geq -2^n$. For a two-qubit pure state ($n = 1, \alpha = 1$), we thus have ${\rm d}_{\max}(\rho_{DQC1}) \leq 1/\sqrt{2}$, which conforms with Eqn. (4). A typical instance of the DQC1 circuit is provided by that of a random unitary U_n in the DQC1 circuit of Fig (1). For such instances of large enough Haar distributed unitaries, ${\rm Tr}(U_n^2)$ is bounded above by a constant with high probability [19]. Thus, the second term inside the square root in Eqn. (12) is approximately zero, and

$${\rm d}_{\max}(\rho_{DQC1}) \approx \frac{\alpha}{2^{(n+1)/2}}. \tag{14}$$

This shows that the DQC1 state experiences very little disturbance under LNU, and in fact this disturbance vanishes asymptotically as n grows. As discussed in the introduction, it would appear that the quantum discord is better suited [13] to quantifying non-classicality in the DQC1 model. This, however, raises the question of how the discord and LNU distance are related, and whether the paradigms of 'disturbance under measurement' and 'disturbance under unitary operations' lead to differing notions of non-classicality. We explore these questions in the following section.

Before closing, for completeness, we invoke Theorem (1) to show that the LNU distance is exponentially decreasing for *any* other choice of bi-partitions A and B of the qubits in ρ_{DQC1}. In fact, since

$${\rm Tr}(\rho_{DQC1}^2) = \frac{1+\alpha^2}{2^{n+1}}, \tag{15}$$

Theorem (1) immediately gives the same upper bound of Eqn. (13).

IV. QUANTUM DISCORD *vs* LNU DISTANCE

Motivated by the fact that both the quantum discord and the LNU distance are aimed at capturing the non-classical features in a quantum state via an induced disturbance, we seek an answer to the question of whether one implies the other in any sense or not. Here, we show that non-zero quantum discord implies a non-zero LNU distance, but that the converse is not necessarily true. We begin with a formal definition of quantum discord.

Given a quantum state $\rho \in D(\mathcal{H}^M \otimes \mathcal{H}^N)$, its quantum mutual information is defined as $\mathcal{I}(\rho) := S(\rho_A) + S(\rho_B) - S(\rho)$. The quantum mutual information can, however, also be defined in an inequivalent way as

$$\mathcal{J}_{\{\Pi_j^A\}}(\rho) = S(\rho_B) - S\left(\rho_{B|\{\Pi_j^A\}}\right) \tag{16}$$

with

$$S(\rho_{B|\{\Pi_j^A\}}) = \sum_j p_j S\left((\Pi_j^A \otimes I^B)\rho(\Pi_j^A \otimes I^B)\Big/ p_j\right),$$

where $p_j = \mathrm{Tr}(\Pi_j^A \otimes I^B \rho)$. Projective measurements on subsystem A removes all non-classical correlations between A and B. The quantity $\mathcal{J}$ thus signifies a measure of classical correlations in the state ρ [12]. To ensure that it captures all classical correlations, we need to maximize $\mathcal{J}$ over the set of one dimensional projective measurements. This leads to the definition of quantum discord [11] as

$$\begin{aligned}\mathcal{D}(\rho) &:= \mathcal{I}(\rho) - \max_{\{\Pi_j^A\}} \mathcal{J}_{\{\Pi_j^A\}}(\rho) \\ &= S(\rho_A) - S(\rho) + \min_{\{\Pi_j^A\}} S\left(\rho_{B|\{\Pi_j^A\}}\right). \quad (17)\end{aligned}$$

Intuitively, quantum discord captures purely quantum correlations in a quantum state. This is distinct from entanglement in the case of mixed states. For pure states, quantum discord reduces to the von-Neumann entropy of the reduced density matrix, which is a measure of entanglement. On the other hand, it is possible for mixed separable states to have non-zero quantum discord. The main theorem concerning the discord that we require here is the following.

Theorem 2 (Ollivier and Zurek [11])**.** *For $\rho \in D(\mathcal{H}^M \otimes \mathcal{H}^N)$, $\mathcal{D}(\rho) = 0$ if and only if $\rho = \sum_j (\Pi_j^A \otimes I^B)\rho(\Pi_j^A \otimes I^B)$, for some complete set of rank one projectors $\{\Pi_j^A\}$.*

We now show the following.

Theorem 3. *For $\rho \in D(\mathcal{H}^M \otimes \mathcal{H}^N)$, if $\mathcal{D}(\rho) > 0$, then $\mathrm{d}_{\max}(\rho) > 0$.*

Proof. We begin by writing ρ in Fano form [20], i.e.

$$\begin{aligned}\rho = \tfrac{1}{MN}\ (&I^A \otimes I^B + \boldsymbol{r}^A \cdot \boldsymbol{\sigma}^A \otimes I^B + \quad (18)\\ &I^A \otimes \boldsymbol{r}^B \cdot \boldsymbol{\sigma}^B + \sum_{s=1}^{M^2-1}\sum_{t=1}^{N^2-1} T_{st}\sigma_s^A \otimes \sigma_t^B).\end{aligned}$$

Here, $\boldsymbol{\sigma}^A$ denotes the (M^2-1)-component vector of traceless orthogonal Hermitian generators of $SU(M)$ (which generalize the Pauli spin operators), $\boldsymbol{r}^A$ is the (M^2-1)-dimensional Bloch vector for subsystem A with $r_s^A = \frac{M}{2}\mathrm{Tr}(\rho_A \sigma_s^A)$, and T is a real matrix known as the correlation matrix with entries $T_{st} = \frac{MN}{4}\mathrm{Tr}(\sigma_s^A \otimes \sigma_t^B \rho)$. The definitions for subsystem B are analogous.

An explicit construction for the generators σ_i of $SU(d)$ for $d \geq 2$ is given as follows [21]. Define $\{\sigma_i\}_{i=1}^{d^2-1} = \{U_{pq}, V_{pq}, W_r\}$, such that for $1 \leq p < q \leq d$ and $1 \leq r \leq d-1$, and $\{|k\rangle\}_{k=1}^d$ some complete orthonormal basis for $\mathcal{H}^d$:

$$U_{pq} = |p\rangle\langle q| + |q\rangle\langle p| \quad (19a)$$

$$V_{pq} = -i|p\rangle\langle q| + i|q\rangle\langle p| \quad (19b)$$

$$W_r = \sqrt{\frac{2}{r(r+1)}}\left(\sum_{k=1}^{r}|k\rangle\langle k| - r|r+1\rangle\langle r+1|\right) \quad (19c)$$

In our ensuing discussion, without loss of generality, for $SU(M)$ we fix the choice of basis $\{|k\rangle\}_{k=1}^M$ above as the eigenbasis [28] of ρ_A.

Assume now that $\mathcal{D}(\rho) > 0$. Then, any choice of complete measurement $\{\Pi_j^A\}$ must disturb ρ, i.e. by Theorem 2, if we define

$$\rho_f := \sum_{j=1}^{M}(\Pi_j^A \otimes I)\rho(\Pi_j^A \otimes I), \quad (20)$$

then $\rho_f \neq \rho$ [11],[12],[22]. Henceforth, when we discuss the action of $\{\Pi_j^A\}$ on ρ_A, we are referring to the state $\sum_{j=1}^M \Pi_j^A \rho_A \Pi_j^A$. Now, let $\{\Pi_j^A\}$ be a complete projective measurement onto the eigenbasis of ρ_A. Then, $\{\Pi_j^A\}$ acts invariantly on ρ_A, and thus must alter the last term in Eqn. (18) to ensure $\rho_f \neq \rho$. To see this, recall that one can write $\rho_A = \frac{1}{M}(I^A + \boldsymbol{r}^A \cdot \boldsymbol{\sigma}^A)$, from which it follows that if $\{\Pi_j^A\}$ acts invariantly on ρ_A, then it also acts invariantly on $\boldsymbol{r}^A \cdot \boldsymbol{\sigma}^A$ from Eqn. (18). Since all generators $\sigma_s^A \in \{W_r\}_r$ are diagonal, it follows that there must exist some $T_{st} \neq 0$ such that $\sigma_i^A \in \{U_{pq}, V_{pq}\}_{pq}$. We now use this fact to construct a LNU U^A achieving $\mathrm{d}(\rho, U_A) > 0$.

Define unitary U^A as diagonal in the eigenbasis of ρ_A, i.e. $U^A = \sum_{k=1}^M e^{i\theta_k}|k\rangle\langle k|$, with eigenvalues to be chosen as needed. Then, $[U^A, \rho_A] = 0$ by construction, and so $U^A \otimes I^B$ must alter T through its action on ρ to ensure $\rho_f \neq \rho$. Focusing on the last term from Eqn. (18), we thus have:

$$\begin{aligned}&\sum_{s=1}^{M^2-1}\sum_{t=1}^{N^2-1} T_{st} U^A \sigma_s^A U^{A\dagger} \otimes \sigma_t^B = \\ &\sum_{s=1}^{M^2-1}\sum_{t=1}^{N^2-1} T_{st}\left(\sum_{m=1}^{M}\sum_{n=1}^{M} e^{i(\theta_m - \theta_n)}\langle m|\sigma_s^A|n\rangle|m\rangle\langle n|\right) \otimes \sigma_t^B\end{aligned}$$

Analyzing each generator σ_s^A case by case, we find, for some $1 \leq p < q \leq M$ or $1 \leq r \leq M-1$:

$$\begin{aligned}&\sum_{m=1}^{M}\sum_{n=1}^{M} e^{i(\theta_m - \theta_n)}\langle m|\sigma_s|n\rangle|m\rangle\langle n| = \\ &\begin{cases}\cos(\theta_p - \theta_q)U_{pq} - \sin(\theta_p - \theta_q)V_{pq} & \text{if } \sigma_s = U_{pq} \\ \sin(\theta_p - \theta_q)U_{pq} + \cos(\theta_p - \theta_q)V_{pq} & \text{if } \sigma_s = V_{pq} \\ W_r & \text{if } \sigma_s = W_r\end{cases}\end{aligned}$$

Denoting by T^f the T matrix for ρ_f, we have:

$$T_{st}^f = \begin{cases}\cos(\theta_p - \theta_q)T_{st} + \sin(\theta_p - \theta_q)T_{wt} \\ \qquad\qquad \text{if } \sigma_s = U_{pq}, \text{ where } \sigma_w = V_{pq} \\ \cos(\theta_p - \theta_q)T_{st} - \sin(\theta_p - \theta_q)T_{wt} \\ \qquad\qquad \text{if } \sigma_s = V_{pq}, \text{ where } \sigma_w = U_{pq} \\ T_{st} \qquad\qquad \text{if } \sigma_s = W_r.\end{cases}$$

Thus, if there exists an s such that $T_{st} \neq 0$ and $\sigma_s^A \in \{U_{pq}, V_{pq}\}_{pq}$, it follows that one can easily choose appropriate

eigenvalues $e^{i\theta_p}$ and $e^{i\theta_q}$ for U^A such that $T^f \neq T$, implying $\mathrm{d}_{\max}(\rho) > 0$. By our argument above for $\mathcal{D}(\rho) > 0$, such an s does in fact exist. □

To show that the converse of Theorem 3 does not hold, we present an example of a zero discord state that has non-zero LNU measure. Consider the two qubit separable state

$$\rho = \frac{1}{2}\left(\frac{I_2 + \boldsymbol{a}.\boldsymbol{\sigma}}{2} \otimes \frac{I_2 + \boldsymbol{b}.\boldsymbol{\sigma}}{2} + \frac{I_2 - \boldsymbol{a}.\boldsymbol{\sigma}}{2} \otimes \frac{I_2 - \boldsymbol{b}.\boldsymbol{\sigma}}{2}\right),$$

where $\| \boldsymbol{a} \|_2 = \| \boldsymbol{b} \|_2 = 1$. This state, by construction, has zero discord for a single qubit measurement on either A or B. To see this, consider the projective measurements

$$\left\{\frac{I_2 \pm \boldsymbol{a}.\boldsymbol{\sigma}}{2}\right\}$$

on A. Let us now study the LNU distance for this state, with the local unitary being applied to say A. Notice that $\rho_A = \rho_B = I_2/2$, and $\mathrm{Tr}(\rho^2) = 1/2$. The former implies that the set of allowed local unitaries is the whole of $SU(2)$, an element of which is given by Eq (11). Let us for convenience parameterize $\boldsymbol{a} = (0, 0, 1)$ and $\boldsymbol{b} = (\sin\gamma\cos\delta, \sin\gamma\sin\delta, \cos\gamma)$. Then, some algebra leads to

$$\mathrm{Tr}(\rho\rho_f) = \frac{1}{2}\cos^2\theta. \tag{21}$$

whose minimum is 0, whereby

$$\mathrm{d}_{\max}(\rho) = \frac{1}{\sqrt{2}}. \tag{22}$$

We thus have an example of a class of separable, zero discord states which demonstrates a non-zero shift under LNU. In fact, it attains the maximum shift possible for two-qubit separable states. Hence, if one wishes to define notions of non-classicality in quantum states in terms of 'disturbance under measurement' versus 'disturbance under unitary operations', and one chooses discord and the LNU distance as canonical quantifiers of such effects, respectively, then the resulting respective notions of non-classicality are not equivalent. As we have shown in Thm. 3, however, the quantum discord is a stronger notion of non-classicality than the LNU criterion.

V. MEASURING CORRELATIONS VIA MEASUREMENT-INDUCED DISTURBANCE

The measure we intend to use in this section was presented by Luo in [16]. It relies on the disturbance of a quantum system under a generic measurement. In that sense, it is similar in spirit to quantum discord, but not quite. In the case of quantum discord, as per Eqn. (17), one maximizes over one-dimensional projective measurements on one of the subsystems. For the new measure, which we will call the measurement-induced disturbance (MID) measure, one performs measurements on *both* the subsystems, with the measurements being given by projectors onto the eigenvectors of the reduced subsystems. Then the MID measure of quantum correlations for a quantum state $\rho \in D(\mathcal{H}^M \otimes \mathcal{H}^N)$ is given by [16]

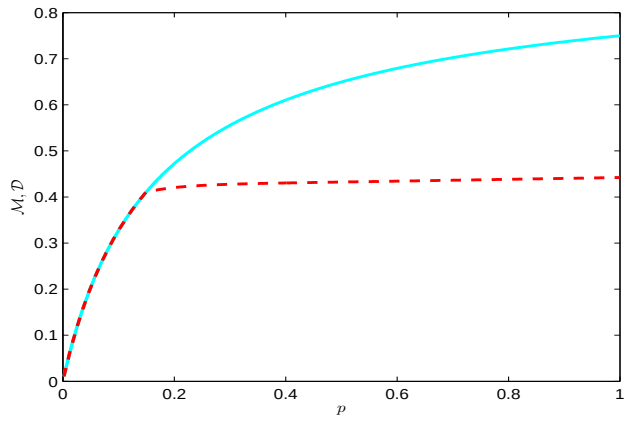

FIG. 2: (Color online) The solid line is the MID measure $\mathcal{M}$ for the 2×4 Horodecki state from [23]. The dashed line is the quantum discord $\mathcal{D}$ for the same state [22]. The kink in the latter curve occurs at $p = 1/7$. We see here, as in the case of the DQC1 state, that the MID measure is greater than or equal to the quantum discord.

$$\mathcal{M}(\rho) := \mathcal{I}(\rho) - \mathcal{I}(\mathcal{P}(\rho)) \tag{23}$$

where

$$\mathcal{P}(\rho) := \sum_{i=1}^{M}\sum_{j=1}^{N}(\Pi_i^A \otimes \Pi_j^B)\rho(\Pi_i^A \otimes \Pi_j^B). \tag{24}$$

Here $\{\Pi_i^A\}, \{\Pi_j^B\}$ denote rank one projections onto the eigenbases of ρ_A and ρ_B, respectively. $\mathcal{I}(\sigma)$ is the quantum mutual information, which is considered to the measure of total, classical and quantum, correlations in the quantum state σ. Since no optimizations are involved in this measure, it is much easier to calculate in practice than the quantum discord or the LNU distance, which involve optimizations over projective measurements and local unitaries respectively. The measurement induced by the spectral resolution leaves the entropy of the reduced states invariant and is, in a certain sense, the least disturbing. Actually, this choice of measurement even leaves the reduced states invariant [16]. Interestingly, for pure states, both the quantum discord and the MID measure reduce to the von-Neumann entropy of the reduced density matrix, which is a measure of bipartite entanglement.

As a nontrivial example, we will consider the well-known Horodecki bound entangled state in $2 \otimes 4$ dimensions [23]. It is bound entangled for all values of $0 \leq p \leq 1$, and the state

is given as

$$\rho_H = \frac{1}{1+7p}\begin{pmatrix} p & 0 & 0 & 0 & 0 & p & 0 & 0 \\ 0 & p & 0 & 0 & 0 & 0 & p & 0 \\ 0 & 0 & p & 0 & 0 & 0 & 0 & p \\ 0 & 0 & 0 & p & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1+p}{2} & 0 & 0 & \frac{\sqrt{1-p^2}}{2} \\ p & 0 & 0 & 0 & 0 & p & 0 & 0 \\ 0 & p & 0 & 0 & 0 & 0 & p & 0 \\ 0 & 0 & p & 0 & \frac{\sqrt{1-p^2}}{2} & 0 & 0 & \frac{1+p}{2} \end{pmatrix}.$$

From this, the projectors onto eigenvectors of the reduced density matrices can be calculated to be

$$\begin{aligned} \{\Pi_1^A, \Pi_2^A\} &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}, \qquad \text{and} \\ \{\Pi_1^B, \cdots, \Pi_4^B\} &= \{ |\Psi^+\rangle\langle\Psi^+|, |\Psi^-\rangle\langle\Psi^-|, \\ &\qquad |\Phi^+\rangle\langle\Phi^+|, |\Phi^-\rangle\langle\Phi^-| \}. \end{aligned}$$

where $|\Psi^\pm\rangle = (|1\rangle \pm |2\rangle)/\sqrt{2}$ and $|\Phi^\pm\rangle = (|0\rangle \pm |3\rangle)/\sqrt{2}$, with $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ forming the computational basis for the second subsystem. Using these in Eqn. (24), we can easily obtain

$$\mathcal{P}(\rho_H) = \frac{1}{1+7p}\begin{pmatrix} p & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & p & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & p & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & p & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1+p}{2} & 0 & 0 & \frac{\sqrt{1-p^2}}{2} \\ 0 & 0 & 0 & 0 & 0 & p & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & p & 0 \\ 0 & 0 & 0 & 0 & \frac{\sqrt{1-p^2}}{2} & 0 & 0 & \frac{1+p}{2} \end{pmatrix}.$$

This density matrix is different from the original one in that there are no coherences between the two subsystems. The MID measure for this state can then easily be obtained analytically as $\mathcal{M}(\rho_H) = S(\mathcal{P}(\rho_H)) - S(\rho_H)$ and is plotted in Fig (2). In the same figure is shown the quantum discord for this state, when a measurement is made on the two-dimensional subsystem. For the details of its calculation, see Ref. [22]. As we see, there are non-classical correlations in this state that are not distillable into maximally entangled Bell pairs. Another instance, dealt with next, is the DQC1 state, which for $\alpha < 1/2$ is, at best, bound entangled, having failed to show any entanglement by partial transposition criterion across any bipartite split. It even failed to show any entanglement at the second level of the scheme of [24]. It therefore might be possible to the quantify the intrinsic information processing abilities of these bound entangled states using the measures dealt with in this paper.

A. MID measure in the DQC1 model

We now move on to calculate the MID measure in the DQC1 model. Our analysis extends that of [16], where only the case of $\alpha = 1$ was considered. Considering $\alpha < 1/2$ here will be of particular interest, due to the lack of distillable entanglement in the DQC1 state. Consequently, we start with the $n+1$ qubit DQC1 state, given by Eqn. (9), wherefrom

$$\rho_A = \frac{1}{2}\begin{pmatrix} 1 & \alpha\tau^* \\ \alpha\tau & 1 \end{pmatrix} \quad \text{and} \quad \rho_B = I_n/2^n. \tag{25}$$

The projectors onto their respective eigenvectors are

$$\{\Pi_1^A, \Pi_2^A\} = \left\{ \frac{1}{2}\begin{pmatrix} 1 & e^{-i\phi} \\ e^{i\phi} & 1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 & -e^{-i\phi} \\ -e^{i\phi} & 1 \end{pmatrix} \right\}$$

where $\tau = re^{i\phi}$ for $r = |\tau|$ is the normalized trace of U_n, i.e. $\tau = \mathrm{Tr}(U_n)/2^n$, and

$$\{\Pi_j^B\} = \{E_j\} \quad \text{where} \quad [E_j]_{kl} = \delta_{kj}\delta_{lj}, \;\; j,k,l = 1, \cdots, 2^n.$$

Using this, we can calculate

$$\begin{aligned} \mathcal{P}(\rho_{DQC1}) &= \sum_{j=1}^{2^n}\sum_{i=1}^{2}(\Pi_i^A \otimes \Pi_j^B)\rho_{DQC1}(\Pi_i^A \otimes \Pi_j^B) \\ &= \frac{1}{2^{n+1}}\sum_j \begin{pmatrix} 1 & \alpha d_j \\ \alpha d_j^* & 1 \end{pmatrix} \otimes E_j \\ &= \frac{1}{2^{n+1}}\begin{pmatrix} I_n & \alpha D \\ \alpha D^\dagger & I_n \end{pmatrix} \end{aligned} \tag{26}$$

where $d_j = (u_{jj}^* + e^{-2i\phi}u_{jj})/2$, with u_{jj} being the (j,j)th entry of U_n, and

$$D = \mathrm{diag}\,(d_1, \cdots, d_j, \cdots).$$

Since D is diagonal, it is fairly easy to obtain the spectrum of $\mathcal{P}(\rho_{DQC1})$, which is given by

$$\boldsymbol{\lambda}[\mathcal{P}(\rho_{DQC1})] = \left\{ \frac{1 \pm \alpha|d_i|}{2^{n+1}} \right\} \quad \text{for} \quad i = 1, \cdots, 2^n. \tag{27}$$

Letting λ_k denote the kth entry of $\boldsymbol{\lambda}[\mathcal{P}(\rho_{DQC1})]$, the von-Neumann entropy of this state is

$$\begin{aligned} S(\mathcal{P}(\rho_{DQC1})) &= -\sum_{k=1}^{2^{n+1}} \lambda_k \log(\lambda_k) \\ &= n + 1 - \frac{1}{2^{n+1}}\sum_{j=1}^{2^n}\Bigg(\log(1-\alpha^2|d_j|^2) \\ &\quad + \alpha|d_j| \log\left(\frac{1+\alpha|d_j|}{1-\alpha|d_j|}\right)\Bigg). \end{aligned} \tag{28}$$

Now,

$$S(\rho_{DQC1}) = n + H_2\left(\frac{1-\alpha}{2}\right), \tag{29}$$

and the entropies of the partial density matrices being identical,

$$\begin{aligned}\mathcal{M}_{DQC1} &= \mathcal{I}(\rho_{DQC1}) - \mathcal{I}(\mathcal{P}(\rho_{DQC1})) \\ &= S(\mathcal{P}(\rho_{DQC1})) - S(\rho_{DQC1}) \\ &= 1 - H_2\left(\frac{1-\alpha}{2}\right) - \frac{1}{2^{n+1}}\sum_i \Bigg(\log(1-\alpha^2|d_i|^2) \\ &\quad + \alpha|d_i|\log\left(\frac{1+\alpha|d_i|}{1-\alpha|d_i|}\right)\Bigg). \end{aligned} \tag{30}$$

Here, $|d_i| = |u_{ii}\cos(\phi+\beta_i)|$ where $u_{ii} = re^{i\beta_i}$ for $r = |u_{ii}|$. Given a unitary, which is known in any implementation of the DQC1 circuit, the above quantity can be computed easily. Not surprisingly, if the random unitary is diagonal, the measure $\mathcal{M}$ for the DQC1 circuit actually reduces to its quantum discord (seen via Eqns. (12) and (13) of [13]). For a Haar distributed random unitary matrix, $|u_{ii}| \sim 1/2^{n/2}$. In the asymptotic limit of large n, $|d_i| \to 0$, in which case the whole quantity within the summation in Eqn. (30) goes to zero. Then,

$$\mathcal{M}_{DQC1} = 1 - H_2\left(\frac{1-\alpha}{2}\right). \tag{31}$$

One fact immediately notable is that the above expression for the MID measure is independent of n, for large n. The result for a $n = 5$ qubit Haar distributed random unitary matrix is shown in Fig (3). As is evident, despite the approximations used in the derivation of Eqn. (31) the asymptotic analytic expression matches the numerical result at $n = 5$ quite well.

The MID measure for the DQC1 state across the bipartite split separating the top qubit from the rest is non-zero for all non-zero values of the polarization. Across this split, the DQC1 state is strictly separable [10] and possesses no entanglement. Hence, it is natural to propose the MID measure as a quantifier of the resource behind the quantum advantage in the DQC1 model [16]. As can be seen from Fig. (3), the behavior of the MID measure is qualitatively quite similar to that of the quantum discord. To argue that one is behind the quantum advantage in the DQC1 model as opposed to the other would be quite premature. Though both these measures attempt to capture the quantum feature of disturbance under measurement, they are quantitatively quite different. We will come back to this point in Section VI.

B. MID measure in quantum communication

We now present an example where the MID measure can be used to interpret the locking of classical correlations in quantum states. It has been shown [17] that there exist bipartite quantum states which contain a large amount of locked classical correlation which can be unlocked by a small amount of

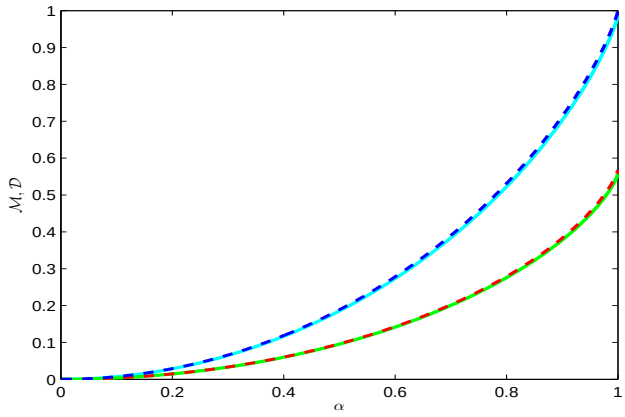

FIG. 3: (Color online) The upper solid (cyan) line is the MID measure $\mathcal{M}$ (Eqn. (30)) for the DQC1 circuit for a $n = 5$ qubit Haar distributed random unitary matrix. The upper dashed (blue) line is the analytic expression for the MID measure for DQC1 states with a Haar distributed random unitary matrix (Eqn. (31)). The lower dashed (red) line shows the discord $\mathcal{D}$ in the DQC1 circuit with the same unitary. The lower solid (green) line shows the analytical expression in of quantum discord from [13]. All quantities are shown as functions of the purity of the control qubit.

classical communication. More precisely, there exist $2n+1$-qubit states for which the optimal classical mutual information between measurement results on the subsystems can be increased from $n/2$ bits to n bits via a single bit of classical communication. Despite the impossibility of this feat classically, the states used in the protocol are not entangled.

Here we use the MID measure to explain this purely quantum phenomenon. To do so, we evaluate the former on a generalization of the state used in [17],

$$\rho = \frac{1}{md}\sum_{k=1}^{d}\sum_{t=1}^{m}(|k\rangle\langle k| \otimes |t\rangle\langle t|)_A \otimes (|b_k^t\rangle\langle b_k^t|)_B, \tag{32}$$

where the set of m orthonormal bases $\left\{\{|b_k^t\rangle\}_{k=1}^{d}\right\}_{t=1}^{m}$ is mutually unbiased (MUB), i.e. $\forall_{t\neq t',i,j}\langle b_i^t|b_j^{t'}\rangle = 1/\sqrt{d}$. As in Ref. [17], when $d = 2^n$ and $m = 2$, the initial correlations in this state amount to $n/2$ bits, and by Alice's sending one bit (the bit t) to Bob, they end up with $n+1$ correlated bits. The state being separable, it has no entanglement. Consequently, we cannot ascribe to it the advantage exhibited by this protocol.

To calculate the MID measure of this state, we need the reduced states given by

$$\rho_A = \frac{I_{md}}{md}, \quad \rho_B = \frac{I_d}{d}.$$

The eigenvectors are trivially obtained, and $\mathcal{P}(\rho)$ is simply the

diagonal of ρ. Thus,

$$\boldsymbol{\lambda}[\mathcal{P}(\rho)] = \frac{1}{md}\{\underbrace{1,\cdots,1}_{d},\underbrace{1/d,\cdots,1/d}_{(m-1)d^2},\underbrace{0,0,\cdots,0}_{d(d-1)}\}$$

whereby

$$S(\mathcal{P}(\rho)) = \log m + (2 - \frac{1}{m})\log d. \tag{33}$$

The spectrum of ρ is given by

$$\boldsymbol{\lambda}[\rho] = \frac{1}{md}\{\underbrace{1,1,\cdots,1}_{md},\underbrace{0,0,\cdots,0}_{md(d-1)}\}$$

which leads to

$$S(\rho) = \log m + \log d. \tag{34}$$

Finally, we have

$$\mathcal{M}(\rho) = S(\mathcal{P}(\rho)) - S(\rho) = \left(1 - \frac{1}{m}\right)\log d, \tag{35}$$

which for $d = 2^n$ and $m = 2$ is the exactly equal to the gain attained by this scheme. Moreover, once Bob receives Alice's bit, the MID measure for their post-communication state drops to 0, the latter being diagonal in a local product basis. This suggests that the MID measure quantifies exactly those non-classical (yet not entanglement-based) correlations in ρ which were initially locked.

A few remarks are in order. Eqn. (35) suggests that a better locking effect is possible for $m > 2$. However, explicit constructions to date using more than two MUBs have been unable to achieve superior locking [18], suggesting that the choice of construction for the MUBs plays an important role. In contrast, Eqn. (35) holds irrespective of the specific choice of MUBs. It is also known that if the bases above are constructed using a large set of random unitaries chosen according to the Haar measure, then the classical mutual information in ρ between Alice and Bob can indeed be brought down to a constant [25]. There is also numerical evidence (Appendix of Ref. [26]) that the dimension of the systems may play a role in achieving better locking. Further connections between locking and the MID measure are being investigated.

Finally, for completeness, we remark that $\mathrm{Tr}(\rho^2) = 1/(2^{n+1})$, and so by Theorem 1, the LNU distance for ρ is bounded by

$$\mathrm{d}_{\max}(\rho) \leq \frac{\sqrt{2^n - 1}}{2^n} \approx \frac{1}{2^{n/2}}. \tag{36}$$

Thus, in contrast to the MID measure, the LNU distance once again reveals vanishing non-classicality with growing n.

VI. CONCLUSIONS

In this paper, we have analyzed two possible quantifiers of non-classical correlations beyond quantum entanglement, specifically locally noneffective unitary operations [14], and the measurement-induced disturbance measure [16], and compared them to the quantum discord [11] within the context of the DQC1 circuit [9].

The LNU distance showed (Eqn. (13)) that there is little non-classicality in the $n+1$ qubit DQC1 state. This behavior is very similar to that of negativity in the DQC1 model which was used to characterize its entanglement [10]. The crucial difference is that the bipartite split chosen in Sec III is separable, and therefore exhibits no entanglement at all. As the LNU distance vanishes exponentially quickly with growing n, one is hard-pressed to relegate the role of the resource exponentially speeding up the DQC1 model to it. Similarly, the LNU distance suggests vanishing non-classicality in the case of locking of classical correlations in quantum states. This does not, however, prove that this kind of quantum characteristic cannot be the resource behind other forms of quantum advantage.

The MID measure, on the other hand, is considerably more satisfactory. The zero-entanglement split in the DQC1 model is shown to have a non-zero amount of non-classicality as per the MID measure. The magnitude of this measure, as shown in Fig. (3), is a constant fraction of its maximum possible value. The maximum possible value, which is independent of the size of the system under consideration, is $\mathcal{M}_{max} = 1$, and is attained for the maximally entangled state. Indeed, for a perfectly pure top qubit $\alpha = 1$, the DQC1 state attains this value. The MID measure can thus be ascribed to be a quantifier of the correlations behind the speedup of the DQC1 model. Indeed, this has already been proposed in [16]. Further, the MID measure also performs well in quantifying non-classicality in the scenario of locking classical correlations in quantum states. The measure, however, lacks a clear physical interpretation of the form of quantum discord, which motivates its operational significance as a measure of pure quantum correlations [27]. Further studies in this direction are required before a comprehensive conclusion can be reached.

Acknowledgements

AD thanks Carl Caves and Anil Shaji for numerous stimulating discussions. AD was supported in part by the US Office of Naval Research (Grant No. N00014-07-1-0304) and also by EPSRC (Grant No. EP/C546237/1), EPSRC QIP-IRC and the EU Integrated Project (QAP). SG was partially supported by Canada's NSERC, CIAR and MITACS. We also thank the anonymous referee for raising certain points that led to improvements in the paper.

[1] R. Jozsa and N. Linden, Proc. Roy. Soc. A **459**, 2011 (2003).
[2] L. Masanes, Phys. Rev. Lett. **96**, 150501 (2006).
[3] D. A. Meyer, Phys. Rev. Lett. **85**, 2014 (2000).
[4] E. Biham, G. Brassard, D. Kenigsberg, and T. Mor, Theor. Comput. Sci. **320**, 15 (2004).
[5] D. Kenigsberg, T. Mor, and G. Ratsaby, Quantum Inform. Comput. **6**, 606 (2006).
[6] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).
[7] A. A. Methot and V. Scarani, Quantum Inform. Comput. **7**, 157 (2007).
[8] A. Ambainis, L. J. Schulman, and U. V. Vazirani, in *STOC* (2000), p. 697.
[9] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).
[10] A. Datta, S. T. Flammia, and C. M. Caves, Phys. Rev. A **72**, 042316 (2005).
[11] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. **88**, 017901 (2002).
[12] L. Henderson and V. Vedral, J. Phys. A **34**, 6899 (2001).
[13] A. Datta, A. Shaji, and C. M. Caves, Phys. Rev. Lett **100**, 050502 (2008).
[14] L. Fu, Europhys. Lett **75**, 1 (2006).
[15] S. Gharibian, H. Kampermann, and D. Bruß, arXiv:0809.4469 (2008).
[16] S. Luo, Phys. Rev. A **77**, 022301 (2008).
[17] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Phys. Rev. Lett. **92**, 067902 (2004).
[18] M. Ballester and S. Wehner, Phys. Rev. A **75**, 022319 (2007).
[19] P. Diaconis, Bull. Amer. Math. Soc. **40**, 155 (2003).
[20] U. Fano, Rev. Mod. Phys. **55**, 855 (1983).
[21] F. T. Hioe and J. H. Eberly, Phys. Rev. Lett. **47**, 838 (1981).
[22] A. Datta, Ph.D. thesis, University of New Mexico, arxiv:0807.4490 (2008).
[23] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
[24] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004).
[25] P. Hayden, D. W. Leung, P. Shor, and A. Winter, Commun. Math. Phys. **250**, 371 (2004).
[26] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, arXiv:quant-ph/0303088 (2004).
[27] W. H. Zurek, Phys. Rev. A **67**, 012320 (2003).
[28] The set of orthonormal eigenvectors of ρ_A will not be unique if the eigenvalues of ρ_A are degenerate. Hence, we fix some choice of eigenbasis for ρ_A as the "canonical" choice to be referred to throughout the rest of our discussion.